PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Thomas Rottschafer et al.
For	:	PROCESSOR FOR ENCRYPTING AND/OR DECRYPTING DATA AND METHOD OF ENCRYPTING AND/OR DECRYPTING DATA USING SUCH A PROCESSOR
Serial No.	:	10/559,917
Filed	:	December 7, 2005
Art Unit	:	2436
Examiner	:	Trong H. Nguyen
Att. Docket	:	DE 030203 US1
Confirmation No.	:	9587

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Pre-Appeal Brief Request is in response to the Office Action dated September 22, 2009, and further to the Notice of Appeal filed concurrently herewith. Applicant hereby requests review of the rejections in the above-identified application in view of the concurrently-filed Notice of Appeal. Claims 1-17 are pending in the present application, of which claims 1 and 11 are independent.

On page 3, the Office Action objects to claims 9 and 16. Applicant is unsure

how to respond to these objections, as they appear to be unrelated to informalities in the claim language. Rather, the Examiner alleges that "the time between calculating . . . and using . . . will normally vary," an issue that appears related to the alleged disclosures in the prior art. Applicant respectfully submits that claims 9 and 16 have no ambiguous language and are clearly supported, for example, by paragraph [0027] in the published version of the specification. Accordingly, Applicant respectfully requests withdrawal of the claim objections.

On pages 3-12, the Office Action rejects claims 1, 2, 4, 10, 11, and 17 under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 5,261,003 to Matsui (hereinafter "Matsui") in view of Application No. US 2003/0202658 to Verbauwhede. On pages 12-16, the Office Action rejects claims 5-9 and 12-16 under 35 U.S.C. § 103(a) as allegedly unpatentable over Matsui in view of Verbauwhede, further in view of secondary references. Applicant respectfully traverses these rejections.

Independent claim 1 recites, in part, the following subject matter: "a first request line that sends requests from the at least one encryption/decryption device to the control device" and "a second request line that sends requests from the round key generator to the control device" (emphasis added). Similar subject matter appears in independent claim 11. Applicant respectfully submits that the references of record, alone or in combination, fail to disclose, teach, or suggest this subject matter.

On page 5, the Office Action correctly concedes that Matsui fails to disclose

the first request line. The Office Action then attempts to remedy this admitted deficiency in Matsui by applying the teachings of Verbauwhede. The Office Action fails to identify either the first request line or the second request line in Verbauwhede. The Office Action only refers to "STATUS" in Fig. 5 of Verbauwhede.

Applicant notes that Fig. 5 of Verbauwhede has a first "STATUS" line that connects an Input FSM [15] to a Main FSM [14]. A second "STATUS" line links an Encryption FSM [19] to the Main FSM [14]. A third "STATUS" line links an Key Scheduling FSM [20] to the Main FSM [14]. A fourth "STATUS" line links an Output FSM [16] to the Main FSM [14]. Applicant respectfully submits that none of these "STATUS" lines are equivalent to the recited first request line because none of the lines send requests from the at least one encryption / decryption device to the control device. None of the FSMs are equivalent to either of the recited devices.

Page 5 of the Office Action alleges that the recited "encryption/decryption device" corresponds to the encryption module [Fig. 2: 10] in Verbauwhede. Page 5 of the Office Action further alleges that the recited "round key generator" corresponds to the key scheduling module [Fig. 2: 12] in Verbauwhede. In response, Applicant respectfully submits that Verbauwhede teaches away from the claimed subject matter because Verbauwhede's encryption module [10] is directly coupled to the key scheduling module [12].

Independent claim 1 recites, in part, the following subject matter: "wherein the at least one encryption/decryption device and the round key generator

communicate solely via the control device" (emphasis added). Similar subject matter appears in independent claim 11. Applicant respectfully submits that the references of record, alone or in combination, fail to disclose, teach, or suggest this subject matter.

On page 4, the Office Action alleges that Matsui discloses this subject matter. In particular, the Office Action alleges that "scramble processing means 33 and address calculating circuit 23 and magnification key latch 7 communicate solely using selector 24, selector 25 (Fig. 1)." In response, Applicant respectfully submits that address calculating circuit 23 is directly coupled to magnification key latch 7. An arrow linking the two boxes is clearly visible in Fig. 1 of Matsui. Moreover, Matsui declares that "[t]he address calculating circuit 23 calculates and [sic] address of a [sic] extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7" (emphasis added). See lines 8-12 of column 2 in Matsui.

Verbauwhede also teaches away from this subject matter. As mentioned above, the Office Action relies upon the encryption [10] and key scheduling [12] modules in Verbauwhede, alleging that they respectively correspond to the recited encryption/decryption device and the round key generator. However, Verbauwhede provides for direct communication between the encryption [10] and key scheduling [12] modules. As depicted in Fig. 2, the key scheduling [12] module sends sub-keys directly into the encryption module [10]. Also, note that "[k]ey scheduling module

12 has to provide on N-bit roundkey per clock cycle to encryption module 10" (emphasis added). See paragraph [0032] of Verbauwhede.

Independent claim 1 further recites, in part, the following subject matter: "wherein the at least one encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines to start the encryption/decryption operation after both requests are met" (emphasis added). Similar subject matter appears in independent claim 11. Applicant respectfully submits that the references of record, alone or in combination, fail to disclose, teach, or suggest this subject matter.

On page 6, the Office Action alleges that "two modules operate in parallel and one round is completed per clock cycle." In response, Applicant respectfully submits that Verbauwhede cannot provide for separate requests from a round key generator and an encryption/decryption device to a control device. Verbauwhede does not start an encryption/decryption operation in response to receiving both requests.

Independent claim 1 recites, in part, the following subject matter: "the control device transmits intermediate results to the round key generator to perform recursive calculation of the at least one round key" (emphasis added). Similar subject matter appears in independent claim 11. Applicant respectfully submits that the references of record, alone or in combination, fail to disclose, teach, or suggest this subject matter.

On page 5, the Office Action correctly concedes that Matsui fails to disclose recursive calculation. In an attempt to remedy the deficiencies of Matsui, the Office Action applies the teachings of Verbauwhede. In particular, the Office Action relies upon paragraph [0032] and Fig. 4a of Verbauwhede.

Paragraph [0032] of Verbauwhede clearly teaches away from the recited subject matter because it involves provision of roundkeys from key scheduling module [12] to encryption module [10]. Fig. 4a does not involve recursive calculation in the claimed manner because Verbauwhede does not have a control device that transmits intermediate results. Moreover, Verbauwhede's teachings cannot be combined with the alleged intermediate results attributed to Matsui to provide a *prima facie* case of obviousness. The bytes of Matsui are not transmitted by the control device and cannot be used in recursive calculations.

Tran, Hennessy, and Muratani fail to remedy the deficiencies of Matsui in Verbauwhede described above. Therefore, Applicant respectfully submits that independent claims 1 and 11 are allowable over the references of record. Claims 2-10 depend from claim 1. Claims 12-17 depend from claim 11. Thus, Applicant respectfully submits that claims 2-10 and 12-17 are allowable at least on the basis of their respective dependencies from allowable claims. Applicant respectfully requests withdrawal of the rejections of claims 1-17 under 35 U.S.C. § 103(a).

In the event the fees submitted prove insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Respectfully submitted,
KRAMER & AMADO, P.C.

Terry W. Kramer

Date: October 22, 2009

Terry W. Kramer
Registration No.: 41,541

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314
Phone: 703-519-9801
Fax: 703-519-9802